

Amendments to the Specification

On page 21, please replace the paragraph beginning on line 8, with the following paragraph:

Turning now to describe in details the different modules of the analyzer 202 illustrated in Fig. 7, it is appreciated that legitimate data conveyed by a node operating in a communication network identifies that node by at least one detectable way. For example, an ARP and/or a RARP packet, basically used for mapping an IP address to its respective MAC (Media Access Control, layer 2) address and *vice versa*, includes at least a MAC address of the sending node (referred to also as the "source node"). Furthermore, in many cases the data includes identification of the data source as well as the data destination. For example, TCP/IP packets typically include identification of the source and destination IP addresses. Thus, the nodes detector ~~702~~ can 701 can analyze each detected datagram (may it be a packet or a higher level message), study its fields in order to identify identifiable nodes, and if one or more of these nodes are not yet recognized by the network information collector, add these nodes to a list of recognized nodes, for example, by creating a record for this node in a database. Alternatively, when the nodes ~~detector 702~~ detector 701 identifies a newly detected node, it can convey its identity to different modules, instead of inserting it to the list of nodes. Fig. 9 is a flowchart illustrating nodes detection, according to one embodiment of the invention.

On page 21, please replace the paragraph beginning on line 3, with the following paragraph:

Before providing detailed description of the modules included in the query engine and suggested embodiments for their methods of operation, it should be ~~realizes~~ realized that it is possible to understand and study information relating to a communication network by querying for information, or in other words, by using measurement traffic, as is already known in the art (see, for example, the articles *"Combining active and passive network measurements to build scalable monitoring systems on the grid"* and *"The Present and Future of Xprobe2, The Next Generation of Active Operating System Fingerprinting"*, mentioned in the background of the invention). The measurement traffic includes packets that are specially constructed, that is, packets whose fields include specific values designed for the purpose of the query. The type and content of the packets is determined in accordance with the queried information that is required, e.g., in accordance with the instructions received from the analyzer 202.